Published and Copyright (c) 1999 - 2003
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Paul Caillet
Kevin Savetz

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
http://www.icwhen.com/aone/
http://a1mag.atari.org
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Another MS Settlement! ~ People Are Talking! ~ Steem Update News!
~ Subpoena Use Protested ~ Ballmer Slams Hackers! ~ New PSX Game Device!
~ 8-bit Graphics Contest ~ OpenOffice 1.1 Ready! ~ Pop-Up Killers!
~ MSBlaster 2 A No-Show! ~ MS Faces Security Suit ~ New AOL Spam Filters

-* P2Ps Unveil Code of Conduct! *-
-* Hackers To Face Tougher Sentences! *-
-* Music Industry Will Talk Before Lawsuits! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, it didn’t take long for us to truly realize that summer was over and fall taken over! While the weather has been nice, it’s getting noticeably colder. Earlier tonight, I pulled in all of my remaining veggies from the gardens to beat the predicted first frost. I had a great crop this year; I’ve been bringing in bagloads of stuff in to work because I can’t keep up with eating it all! And some of my neighbors have also been getting some. But, that’s over for another season.

We’re finally getting that addition to the house next week. Actually, we’re enclosing our existing deck with a sunroom, but it will be almost like adding an additional room to the house. That should be fun, especially in the warmer months.

Things at work are still hectic as ever. I could rant about it for pages, but I won’t. I’m sure that many of you have had similar experiences in the past. Wouldn’t it be nice to be back in simpler times, like when using an Atari computer was a breeze rather than messing with more complicated machines.

On a happier note, if you recall my relating the story of "Pug" last week, he’s back home from the veterinary hospital. He seems to be recovering well, but still has a way to go. Still, it’s heartening to know he’s back home with family. that will help to speed up the healing process.

Until next time...

=~=~=~=

Steem 2.61

Hello,

26th September 2003 - Steem v2.61

Well v2.5 didn’t contain any major bugs, but v2.6 did. So here is a

small update to stop Steem crashing, there are no emulation improvements. However this version is definitely worth the download as, thanks to the author of Netatari (rb), we have finally fixed the Windows 98 extended features crash, so now all Steem users have access to the profiles and macros features.

Bugs

. Fixed extended features Windows 98 crash finally (thanks rb!)
. Stopped crashing on complex 60Hz screens
. Corrected extended monitor reset display

New Features

. Close disk manager after insert, reset and run option
. Australian keyboard language added
. DEBUG: Added I/O address monitoring, write and read

You can get the update from the download page:
http://www.blimey.strayduck.com/download.htm

Best regards,
Paul CAILLET

## $500 Atari 8-bit Graphic Programming Contest

Mark DiLuciano of Sunmark Products has announced a $500 Graphic Programming Contest for Atari 8-bit computers. All you need to do is deliver an executable that can be loaded on an 8-bit machine, with a maximum file size of

16K. First prize is $300 cash, second prize $150, and third prize $50. The art can be on any subject matter, and can even be animated. The contest will run until October 20th, 2003, with winners announced on November 1st. For complete details, visit:

http://www.atariage.com/forums/viewtopic.php?t=34470

=~=~=~=

## PEOPLE ARE TALKING

compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. It’s gonna be a short column this week. I’ve got some kind of flu bug, and I feel like hell. It’s not the worst sickness I’ve ever had... I didn’t even miss work today. Although I wish I had been smart enough to stay home. I think that, more than anything else, it annoys me to be sick. And at the same time that I’m annoyed by being sick, I’m happy that it’s just a case of the flu.

Well, let’s get on with the news, hints, tips, and info available from the

UseNet.

>From the comp.sys.atari.st NewsGroup
==========

Facundo Arena asks about a parallel port driver:

"I'm looking for a Parallel-port-drive driver called HDD-Daemon, which may let me use a PC HDD on my Atari 1040STfm, using a special parallel port cable. Does anyone have it? Is it good? It seems the be the only option I have since it's impossible for me to find a SCSI host adapter or something like that...."

Adam Klobukowski tells Facundo:

"Search for hdd_dmn .lzh or .zip. I remember there was page in czech language with it."

Facundo checks around and tells Adam:

"I found it! Thanks!!! Now, do I have to build a special parallel cable? I think my PC has a bidirectional parallel port... is it necessary?"

'Bruce' asks a favor of Facundo:

"Could you post the link to the files ?
i'm trying to get my ST a hard disk too.....
And maybe, i can help you on building that cable!

Nevermind...
i found it...

I was reading...
And off course, you will need a bi-dir parallel port..
(But, all newer computers are equipped with, at least, one)
The problem, is to build the cable.
nothing else..
I'm going to build it, and post comments.."

Kenneth Medin asks about Adamas with STiNG and a little twist:

"I'm trying out the Adamas browser using a STinG setup with the Draconis emulator. I'm on a LAN with EtherNec and a "broadband router" with NAT connected to the Internet.

Using Adamas strictly locally on the LAN I can surf to both the Weblight web server on another Atari here and a pc running Debian/Apache. But as soon as there is a single link to the outside with a named url (a counter for example) Adamas goes down. If I try to enter an external url it goes down right away.

Apart from that Adamas seems to be quite a nice browser but useless to me at the moment...

When I try to Ping other hosts with DRACPING.PRG I get response from all computers on my LAN including the router. If I Ping any outside numerical address I get no response at all! Judged by the lights on the router the Ping packets does not even manage to go through the NAT of my router and out on the Internet. Resolving works OK as there is a DNS proxy in the router.

All native STinG clients work like they should.

Has anyone managed to Ping an outside host using Draconis on a similar setup?

I find it interesting that Adamas crashes on all external sites but not on local 192.168.0 LAN sites and DRACPING.PRG fails to reach the same sites."

Edward Baiz offers this bit of info to Kenneth:

"I got it to work with my Lan using MagicNet. Have not tried the Mint side, but I would guess it would work also...."

John Garone asks an interesting question about forging message headers:

"How much of a header can be forged? It seems to me you can’t forge the IP #s which the post or mail passes through so shouldn’t they be traceable back to the real source?"

Guy Harrison tells John:

"Let’s find out shall we? I’m using my ISP’s mail server here ’cos my local one would insert lots of stuff and wouldn’t get the point across...

```
$ telnet smtp.ntlworld.com 25
Trying 62.253.162.40...
Connected to smtp.ntlworld.com.
Escape character is ’^]’.
220 mta03-svc.ntlworld.com ESMTP server (InterMail vM.4.01.03.37
201-229-121-137-20020806) ready Sun, 28 Sep 2003 17:29:17 +0100
helo
250 mta03-svc.ntlworld.com
helo atlantik.net
250 mta03-svc.ntlworld.com
mail from: foo@atlantik.net
250 Sender <foo@atlantik.net> Ok
rcpt to: swamp-DEL-dog@ntlworld.com
250 Recipient <swamp-DEL-dog@ntlworld.com> Ok
data
354 Ok Send data ending with <CRLF>.<CRLF>
From: John Garone <swamptax-NOT-@atlantic.net>
To: Mr IRS Dude@irs.com
Subject: Dat darn bill

I will not pay! No, not ever!!!
.
250 Message received: 20030928163141.TXFQ27049.mta03-svc.ntlworld
com@atlantik.net
```

```
quit
221 mta03-svc.ntlworld.com ESMTP server closing connection
Connection closed by foreign host.
```

The only thing I altered above is to insert "-DEL-" so that spambots can't grab me address off this article. Lo & behold the end-product appears moments later...

```
Return-Path: <foo@atlantik.net>
Received: from atlantik.net ([80.4.128.70]) by mta03-svc.ntlworld.com
          (InterMail vM.4.01.03.37 201-229-121-137-20020806) with SMTP
          id <20030928163141.TXFQ27049.mta03-svc.ntlworld.com@atlantik.net>
          for <swamp-DEL-dog@ntlworld.com>; Sun, 28 Sep 2003 17:31:41 +0100
From: John Garone <swamptax-NOT-@atlantic.net>
To: Mr IRS Dude@irs.com
Subject: Dat darn bill
Message-Id: <20030928163141.TXFQ27049.mta03-svc.ntlworld.com@atlantik.net>
Date: Sun, 28 Sep 2003 17:32:45 +0100
Status: R
X-Status: N
X-KMail-EncryptionState:
X-KMail-SignatureState:

I will not pay! No, not ever!!!
```

Okay, so what's useful there. Not much I'm afraid. If you want to report someone then this is the line...

```
atlantik.net ([80.4.128.70]) by mta03-svc.ntlworld.com
```

...and ignore the textual address. As you can see that's bollox as well. It's the IP address you're after...

```
$ nslookup 80.4.128.70
Server:  cache1.ntli.net
Address:  194.168.4.100
Name:    m70-mp1.cvx1-a.not.dial.ntli.net
Address:  80.4.128.70
```

...and a...

```
$ whois  80.4.128.70
[snip lots of stuff]
```

...ought to yield an ISP address to report it to. You don't need these tools on your machine: there's plenty of web based ones. Note that there's a clue in the above "Name:" that its a dialup account & therefore pretty certain to be on a dynamic address. You need ISP help to discover who was using that address at the time of the abuse. However, if it does happen to be a fixed address then you're laughing so to speak 'cos it identifies them directly."

David Bolt adds his thoughts:

"Any header in a mail can be forged, with the exception of those inserted by the last server to handle the mail (should only be a Received: header, but some broken clients don't insert a Date: header). In general, these are going to be the ones added by your ISP, or your own server if your running

one.

Here’s a tutorial on how to read headers:

<URL:http://www.stopspam.org/email/headers/headers.html>

Google throws up a few more links with this:

<URL:http://www.google.com/search?q="help%20reading%20headers">

Searching Google groups should turn up a few more, but it looks like Google groups has a problem with memory. It seems to have forgotten stuff from the last 4 or 5 years."

’Yves’ asks about setting up EasyMiNT:

"I’m trying to install Easymint on a good old Atari STE with SCSI HD connected to ICD LINK.
I set up the HD with 3 partitions using atari-fdisk under linux:
*/dev/sda1 10MB GEM boot partition
*/dev/sda2 190MB LNX partition
*/dev/sda3 50MB BGM partition (for Easymint installer)

I use ICD drivers to make my HD recognized by the Atari, but it seems only both GEM and BGM partitions are seen from this drivers!
So when I launch the easymint installer, i’m logically told no LNX or RAW partition is found on my HD.
I tried using CBHD drivers instead of ICD drivers, but all I can get at boot time is 4 bombs and of course, no desktop.

My questions are:
*is CBHD able to see LNX partitions so that i can install Easymint ?
*how can I make CBHD stop to crash at boot?
*(worst case) do I really _need_ to buy HDDRIVER if everything fails? How can I be sure it will work on my system, since demo version doesn’t have SCSI driver target interface and allows writing only  C: ?"

Maurits van de Kamp tells Yves:

"So, all this under a big "IIIC" (If I’m Informed Correctly) :

MiNT extended file systems require XHDI, which is (I think) an API extension to the hard disk driver. I know that the ICD drivers don’t have this, I don’t know about CBHD. HDDriver does for sure. And it’s the best hard disk driver anyway, so use it

However, I don’t know if this is the cause of the fact that the driver doesn’t actually see the partitions. I would expect them to see them, just MiNT not being able to use XFS-drivers."

Lonny Pursell adds:

"I am quite sure the latest minixfs driver requires XHDI.
It would be safe to assume the other extended file systems do as well."

Yves adds:

"Oh well, HDDRIVER seems to be ok, but it's a commercial software, and I believe that paying for a driver to install a free OS is quite a paradox! My ST can't match with nowadays PCs and MACs productivity and still I have to spend 35 EUR for just having _free_ fun with an obsolete computer? That's why I try harder with CBHD, as it is freeware and said to support XHDI... But I didn't find yet any info on how to configure it to make it see LNX partitions..."

Lonny tells Yves:

"I can only recall my setup of minix. When I did this, I had to partition the drive, then set the partition type as RAW if I remember correctly. Once I did that, the minix setup tool would see it and setup the partition for use. I already had the commercial driver at the time though.

You might try finding a used copy at a reduced cost or watch ebay."

Well folks, my meds are wearing off and my wife (aka 'The Ball & Chain') is telling me I need to rest. I'll be past this wee lil' beastie in the next day or so, so tune in next week and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - PS2 Price Cut In UK!
New All-In-One PSX Device!
Half-Life 2 Woes!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Sony Cuts PlayStation 2 Price in UK for Christmas Push

Sony Corp said on Tuesday it would drop the price of its best-selling PlayStation 2 video game console in the United Kingdom, the first price cut in over a year in the company's top European market.

Beginning October 1, the PlayStation will carry the suggested retail price of 139 pounds ($232.40), representing a 13 percent discount, the company said.

"We’re bringing the UK in line with a price cut the rest of Europe had earlier in the year. The UK was the only territory where the price remain unchanged," a spokesman for Sony Computer Entertainment Europe said.

In continental Europe, PlayStation 2 has a suggested retail price of 199 euros ($233.20). Sony cut prices in continental Europe and the U.S. in May in preparation for a traditionally slow summer retail season.

Demand in the U.K. has remained relatively strong, enabling the company to maintain prices at the higher level for a longer period.

Rumors persisted that Sony would be forced to introduce discounts for the Christmas period to match prices of its trailing rivals Microsoft Corp’s Xbox and Nintendo’s GameCube.

## Sony to Unveil All-In-One PSX Game Device Next Week

Sony Corp said on Friday it would unveil its all-in-one PSX game device to the public next week.

The PSX, which packs a TV tuner, DVD recorder, hard-disk drive, and the PlayStation 2 game player into a single white box, will be unveiled at the CEATEC Japan 2003 industry show in Makuhari, near Tokyo, on Tuesday, Sony said in a statement.

Sony plans to launch the machine in Japan before the end of this year, and in Europe and the United States early next year, but a spokesman for Sony said on Friday the exact launch timetable and pricing were yet to be decided.

Some analysts have expressed concerns the PSX could eat into demand for other Sony products at a time when the company is suffering from sluggish sales of its Vaio PCs and home electronics goods.

## IE Gets Blame for Theft of Half Life 2 Code

Security experts are blaming known but unpatched vulnerabilities in Microsoft Corp.’s Internet Explorer for the theft and distribution of the source code for a much anticipated new video game.

The source code for Valve Corp.’s Half Life 2, a sequel to the popular shoot-’em-up game that was due out by December, was posted on the Internet on Thursday, according to a statement from Valve Managing Director Gabe Newell. The theft of the code, which was made available for download on the Net, came after a monthlong concerted effort by hackers to infiltrate Valve’s network. Malicious activity in the Valve network included denial-of-service attacks, suspicious e-mail activity and the installation of keystroke loggers, Newell added.

"This is what happens when you have 31 publicly known unpatched vulnerabilities in IE," wrote Thor Larholm, senior security researcher for PivX Solutions LLC, in a posting to the NTBugTraq mailing list. "I have seen screenshots of successfully compiled HL2 installations, with WorldCraft and Model Viewer running atop a listing of directories such as

hl2, tf2 and cstrike."

Newell is seeking the Internet and gaming communities' help in tracking down the code thieves. The company has set up an e-mail address, helpvalve@valvesoftware.com, to collect information and tips on the hack.

## Military Recruits Video Game Makers

Hunched with his troops in a dusty, wind-swept courtyard, the squad leader signals the soldiers to line up against a wall. Clasping automatic weapons, they inch single-file toward a sandy road lined with swaying palm trees.

The squad leader orders a point man to peer around the corner, his quick glance revealing several foes lying in wait behind a smoldering car. A few hand signals, a quick flash of gunfire, and it's over.

The enemy is defeated, but no blood is spilled, no bullet casings spent: All the action is in an upcoming Xbox-based training simulator for the military called "Full Spectrum Warrior."

Increasingly, the Pentagon is joining forces with the video games industry to train and recruit soldiers. The Army considers such simulators vital for recruits who've been weaned on shoot 'em up games.

Even the Central Intelligence Agency is developing a role-playing computer simulation to train analysts.

"We know that most of our soldiers know how to use a game pad," said Michael Macedonia, chief scientist at the Army's Program Executive Office for Simulation, Training and Instrumentation in Orlando, Fla. "Every kid figures out the controls pretty fast."

For years, the U.S. armed forces have used big, sophisticated simulators with hydraulics, wall-sized video screens and realistic cockpits. But such gear costs millions of dollars - far too pricey even by military standards to be widely available.

And that's why video games make sense.

"Full Spectrum Warrior" was created through the Institute for Creative Technologies in Marina Del Ray, Calif., a $45 million endeavor formed by the Army five years ago to connect academics with local entertainment and video game industries. The institute subcontracted game development work to Los Angeles-based Pandemic Studios.

The institute's other training program, "Full Spectrum Command," was released for military use in February.

That game, for the PC, is geared toward light infantry company commanders who lead about 120 people. Set in eastern Europe, it tests organization, decision-making and the ability to recognize threats in a peacekeeping setting.

With "Full Spectrum Warrior," currently in testing at Fort Benning, Ga., squad leaders learn how to command nine soldiers in complex, confusing urban warfare scenarios. The game isn't not about sprinting, Rambo-like, through alleys with guns blazing.

"It’s not really about shooting at things," Macedonia said. "Learning how to shoot your weapon is easy. The challenging thing is leading."

The game the Institute for Creative Technologies has been working on with the CIA for about a year - at a cost of several million dollars - will let agency analysts assume the role of terror cell leaders, cell members and operatives.

"Our analysts would be accustomed to looking at the world from the perspective of the terrorists we are chasing, and learn to expect the unexpected," CIA spokesman Mark Mansfield said.

Training aside, video games are increasingly viewed by top brass as a way to get teenagers interested in enlisting.

Games such as "America’s Army", developed and published by the Army, and "Guard Force", which the Army National Guard developed with Alexandria, Va.-based Rival Interactive, can be downloaded or picked up at recruitment offices.

"America’s Army" has been a hit online since its July 2002 release, attaining some 1.5 million registered users who endure a basic training regiment complete with barbed-wire obstacle courses and target practice.

"Guard Force" has been less successful.

Released last year, features bland synth-rock music that blares in the background. Between video commercials touting the thrills of enlisting in the Army National Guard, gamers pluck flood victims from rooftops or defend a snowy base. In the training mission, gamers deploy helicopters, even tanks, to rescue skiers trapped in an avalanche.

The creators of "Full Spectrum Warrior" hope their stint with the Army will also spur commercial sales.

Pandemic is already busy creating a retail version that will add multiplayer capability, streamline the controls and dispense with such realities as death from a single gunshot wound.

"The explosions will be bigger. Smoke will develop more quickly. A squad leader could call in an F-16 strike," said Jim Korris, creative director for the Institute for Creative Technologies. "That doesn’t happen in the real world."

THQ Inc. is expected to release the public version early next year. An early demonstration in May at Electronic Entertainment Expo, the video game industry’s annual trade show, won "Best Original Game" and "Best Simulation" awards.

There are no plans to commercially release the CIA game.

=~=~=~=

Compiled by: Dana P. Jacobson

# MSBlaster II Fails To Materialize, Worm Writers Lying Low

Over a week ago, several security experts noticed that exploit code for a recently-disclosed vulnerability in Microsoft Windows was circulating throughout the hacker underground, and said that another MSBlaster-style worm was only "days away."

No such worm appeared. What gives?

"We saw a highly functional binary that exploited Microsoft 2000 and evidence of tools that would allow an attack on Windows XP," said Ken Dunham, an analyst with security firm iDefense, and one of those who claimed that a so-called MSBlaster II worm was imminent. On further analysis, it turned out that the code was buggy, and didn't always work.

"It's hard to predict what's out there," Dunham said in defending the announcement of an imminent MSBlaster II worm. "But security firms do understand trends. We have a good understanding of the hacker underground, and we were seeing a ton of activity on the 039 vulnerability. We really thought that something was going to happen."

Another of the security experts who said that another MSBlaster worm might show up soon was Bruce Schneier of Counterpane Internet Security.

"So far we're lucky," he said. "But this stuff is all random. Worms are created by the kind of guy who when he doesn't have a date, writes a worm.

"It's a judgment call," Schneier said, in talking about whether to make an announcement or keep quiet. "You're right, people get complacent," when you make constant announcements, "but the real problem is that there are so many patches and vulnerabilities. You just do the best you can."

Dunham defended the practice of blowing the whistle on possible worms. "Getting the news out has a side benefit of getting a lot of people to update, people such as home users and small businesses who don't normally update regularly. It helps protect a lot of computers against vulnerabilities."

Other security experts agreed that spreading the warning about a potential new worm was the right thing to do. At least in this case.

Other security experts agreed that spreading the warning about a potential new worm was the right thing to do. At least in this case.

"They were absolutely correct, and would have been remiss if they hadn't," said Alfred Huger, the senior director of engineering at Symantec's security response center. "Unfortunately, we don't always nail a time window on an exploit," he explained. Although there's a danger of destroying credibility in the long term by 'crying wolf,' Huger noted that there's a very fine line between disclosing that an exploit exists and saying nothing. Security firms can get slammed either way.

"Security vendors have to be remarkably careful about disclosing information, but in this case, it was based on pretty solid information."

It may be that worm writers are playing possum, spooked by recent arrests in both the U.S. and Romania of men charged with writing variants of the original MSBlaster. Dunham and Huger said that these arrests might well be the reason why a new worm hasn't shown.

"The people who create worms are lying low," Dunham said. "When worm authors are quickly prosecuted and held accountable, that impacts development. They're thinking, 'It's just not worth it if I'm going to jail.'"

"I think they saw the arrests and decided writing a worm wasn't worth the trouble," Huger agreed.

Not that there isn't plenty of hacker activity related to the second RPC DCOM vulnerability in Microsoft Windows. That vulnerability goes by the Microsoft-assigned moniker of MS03-039.

"We're still seeing hard evidence that a significant number of computers have been infected by Trojan horse authors exploiting the 039 vulnerability," Dunham said. "They're still targeting computers that are vulnerable."

The behind-the-scenes activity is both different, and possibly more dangerous, than an actual worm, Dunham said.

Trojan horse authors can very quietly and covertly attack systems with the intention of remotely controlling them, then use that access to steal confidential information from compromised machines. Their motivation differs from that of worm authors, who simply want to see the Internet disrupted on a massive scale.

But even though another MSBlaster hasn't struck, that doesn't mean users should be complacent, Dunham said.

"Trojan horse authors are continuing their attacks," he said.

## Hackers to Face Tougher Sentences

Convicted hackers and virus writers soon will face significantly harsher penalties under new guidelines that dictate how the government punishes computer crimes.

Starting in November, federal judges will begin handing out the expanded penalties, which were developed by the U.S. Sentencing Commission. Congress ordered the changes last year, saying that sentences for convicted computer criminals should reflect the seriousness of their crimes.

"The increases in penalties are a reflection of the fact that these offenses are not just fun and games, that there are real world consequences for potentially devastating computer hacking and virus cases," said John G. Malcolm, deputy assistant attorney general and head of the U.S. Justice Department's computer crimes section. "Thus far, the penalties have not been commensurate with the harm that these hacking cases have caused to real victims."

There are multiple factors that a judge depends on to determine whether to send someone to prison and for how long, but most maximum prison sentences

handed down for computer crime range from one year to 10 years. Hackers whose exploits result in injury or death - if they disable emergency response networks or destroy electronic medical records, for example - face 20 years to life in prison.

Hackers will face up to a 25 percent increase in their sentences if they hijack e-mail accounts or steal personal data - including financial and medical records and digital photographs. Convicted virus and worm authors face a 50 percent increase.

Sentences also will increase by 50 percent for hackers who share stolen personal data with anyone. The sentences will double if the information is posted on the Internet. More than half of the sentences handed out under federal computer crime laws would be lengthened by this change alone, according to a Sentencing Commission report released in April.

Jail time also will double for hackers who break into government and military computers or networks tied to the power grid or telecommunications network.

Hackers who electronically break into bank accounts can be sentenced based on how much money is in the account, even if they don't take any of it. Under the new guidelines, however, judges can tack on a 50 percent increase to the sentence if the hacker did steal money.

Prosecutors traditionally had to show that computer criminals caused at least $5,000 in actual losses to win a conviction. The new guidelines let victims tally financial loss based on the costs of restoring data, fixing security holes, conducting damage assessments and lost revenue.

"Some computer crimes are more serious than others, and these new guidelines reflect that critical infrastructures need to be protected and that invasions of privacy need to be treated as seriously as invasions of our pocketbooks," said Mark Rasch, former director of the Justice Department's computer crimes division and chief security counsel for Solutionary Inc., an Internet security company in Tysons Corner, Va.

Kevin Mitnick, a well known former hacker who spent almost six years in prison, said he doubts the increased penalties would deter hackers.

"The person who's carrying out the act doesn't think about the consequences, and certainly doesn't think they're going to get caught," Mitnick said. "I really can't see people researching what the penalties are before they do something."

The new guidelines will not apply to sentences handed out or prosecutions underway before Nov. 1. This includes the high-profile case of Adrian Lamo, the 22-year-old computer hacker who stands accused of infiltrating and damaging the New York Times Co.'s source list and computer network.

In addition, the guidelines generally will not apply to juveniles, who normally are charged in state courts. In one notable exception, the government last week charged a North Carolina youth as an adult for releasing a version of the Blaster worm.

Most computer criminals are well educated, have little or no criminal history, commit their crimes on the job and often are seeking financial gain, according to Sentencing Commission documents. Of the 116 federal computer crime convictions in 2001 and 2002, about half involved disgruntled workers who used their knowledge to steal from or to discredit

their former employers.

Jennifer Granick, an attorney who represents one of those criminals, said that they are unfairly singled out for tougher sentences than other white-collar perpetrators.

"In most cases, the use of a computer is the trigger for prosecution or for greater sentencing, because so many upward adjustments apply once a computer is involved in the case," said Granick, director of Stanford Law School's Center for Internet and Society.

Her client is Bret McDanel, a 30-year-old California man sentenced in March to 16 months in prison for revealing sensitive security information about his former employer's computer network. Federal prosecutors said McDanel, who worked as a computer security staffer for the now-defunct Tornado Development Inc., sent the information to Tornado's 5,000 customers in September 2000, crashing the company's server.

McDanel would have faced two years in jail under the new sentencing guidelines, said Granick, who argued that it is difficult to place a real dollar loss on computer crimes so judges typically impose harsher sentences than necessary.

Granick also said prosecutors could manipulate the damage amount to appear much larger than it really is, giving the government an advantage in plea bargaining.

Malcolm, the Justice Department's computer crimes chief, said that the department does not give prosecutors suggestions on determining damage amounts, and that prosecutors pursue plea bargain negotiations on a case-by-case basis.

Internet security expert Rasch said that the number of computer-related prosecutions could rise as federal prosecutors try to tie them into otherwise unrelated crimes. He said this is especially possible in light of a recent memo from Attorney General John Ashcroft urging prosecutors to seek more convictions and stronger sentences based on the most serious charges they can find.

"We could soon end up seeing a greater number of ordinary crimes prosecuted as computer crime in an effort to get more leverage for a plea, just because somehow, somewhere there's a computer involved," Rasch said.

Malcolm said this is unlikely.

"In your run-of-the-mill cases where the computer is only a tangential part of the crime, there are not going to be significant enhancements," he said.

If there is an increase, he added, it is because "whether they're drug dealers, embezzlers, hackers or software pirates... people who commit crimes use computers more than they used to."

## Peer-To-Peer Networks Unveil Code of Conduct

Several Internet "peer-to-peer" networks unveiled a code of conduct on Monday to encourage responsible behavior among the millions of users who copy music, pornography and other material from each others' hard drives.

The networks also asked Congress to figure out some way that recording companies and other copyright holders can be reimbursed for the material traded online and urged users to get involved.

The recording industry, stung by declining CD sales that it attributes to widespread peer-to-peer use, has taken the software makers and more recently their users to court in an attempt to squelch the practice.

The Recording Industry Association of America, which represents the five largest labels, said Monday it had reached settlements with 64 of the 261 individuals they sued earlier in September, usually for less than $5,000.

In an attempt to drum up political support, the RIAA has also portrayed peer-to-peer networks as a dangerous haven for child pornographers, identity thieves and "spyware" that secretly tracks online activity.

Such charges "are not central to the relevant debate, and that debate is about how we build an online marketplace for the 21st century," said Adam Eisgrau, executive director of P2P United, an industry trade group.

P2P United members - Lime Wire, Grokster, Blubster, BearShare, Morpheus and eDonkey 2000 - said they would help law enforcers track down child pornographers, would make it easier for users to protect sensitive material on their hard drives, and would not secretly install spyware on users' computers.

The group also said it would encourage users to learn about copyright laws but would not install filters or otherwise limit users' ability to trade copyrighted material. Such filters would not be technically feasible and would infringe on legally permitted methods of sharing, they said.

Kazaa, the music file-sharing service that is the most widely used peer-to-peer network, is not a member of the group.

P2P United invited the recording companies to sit down and negotiate a method so they could be paid for the copies users make of their materials. Members suggested various models such as the per-song fee radio stations pay song publishers or the small surcharge levied on blank video and audio tapes, but steered clear of specifics.

As was the case with radio, the videocassette and other technologies that have eventually enriched Hollywood, content owners have more to gain from negotiation rather than litigation, they said.

"Music is what it is in big part because of radio," said Pablo Soto, chief executive of the Blubster network.

An RIAA spokeswoman said it was "refreshing" to see P2P United educate its users about copyright law and security risks.

"But let's face it, they need to do a whole lot more before they can claim to be legitimate businesses," RIAA spokeswoman Amy Weiss said in a statement.

## Use of Subpoenas to Name File Sharers Criticized

The music industry’s ability to use subpoenas to learn the names of people who allegedly pirate songs over the Internet is coming under increasing fire from civil liberties groups and members of Congress concerned at how the power is being employed to launch a broad legal attack on file sharing.

The Digital Millennium Copyright Act of 1998 gives copyright holders wide latitude to demand that Internet service providers turn over the names and addresses of people suspected of illegally trading song files.

Over the summer, lawyers for the music industry - under the umbrella of its trade group, the Recording Industry Association of America - used that power to serve more than 1,500 "information subpoenas" on phone and cable companies and other Internet providers in an attempt to learn who owned the Internet accounts belonging to the users of file-sharing services.

With that information, the industry filed lawsuits against 261 people on Sept. 8, and it has promised thousands more suits are coming.

The music industry said it needed to take the action to slow the free sharing of digital music over the Internet, a trend it blames for a 31 percent slump in sales over the past three years. But the industry’s aggressive use of the subpoenas has drawn the ire of Internet service providers, which believe it violates their customers’ privacy, and some lawmakers, who blanche at seeing children and grandparents getting sued by powerful commercial interests. A Senate hearing on the subject is scheduled for today.

Monday, the American Civil Liberties Union asked a federal court to quash one of the RIAA’s subpoenas that would force Boston College to hand over the name of a female senior whom the RIAA suspects of pirating songs.

The ACLU calls the information subpoena unconstitutional, saying it violates due process, and filed the motion to quash on behalf of student "Jane Doe."

For others, the RIAA suits look heavy-handed.

"The bottom line is, there has got to be a better way" than mass-suing file sharers, said Sen. Norm Coleman (R-Minn.), who will chair a hearing today of the Senate Permanent Subcommittee on Investigations, featuring testimony from Jack Valenti, president of the Motion Picture Association of America, and new RIAA Chairman Mitch Bainwol, in his first high-profile public appearance.

Coleman noted that copyright law allows for fines as high as $150,000 per violation, or, essentially, per traded song or movie file, and that defendants in the suits may not have known that friends or children were using their computers.

The RIAA withdrew one suit after the target said her computer did not run the right software for file sharing. But the industry said it had settled 64 other suits. In an interview last week, RIAA President Cary Sherman said the settlements are averaging about $3,000 per defendant.

"I come back to basic concerns about how the industry is making an example of a few people using broad power that is essentially unregulated," said Coleman, who added that his 17-year-old son traded songs online until Coleman told him to stop. "It puts people in fear of draconian penalties to settle up on something they may or may not have done."

Verizon Communications Inc., the nation’s largest phone company, was at the table when the Digital Millennium Copyright Act was drawn up and the information subpoena agreed upon.

But Verizon had second thoughts about the provision earlier this year and said it would not hand over its customers’ names to the RIAA. In April, the U.S. District Court in Washington ruled against Verizon, saying it must comply with the federal law. Verizon has appealed the decision, which is being considered by the U.S. Court of Appeals in Washington.

"In hindsight, it was a mistake to agree to it," said Sarah B. Deutsch, Verizon’s associate general counsel. "We thought it would be rarely used."

The information subpoena does not require a judge’s order but merely a clerk’s stamp and a small payment. For a time this summer, the RIAA turned a small office at the U.S. District Court on Constitution Avenue into a subpoena factory, as clerks were brought in from adjacent offices to keep up with the association’s appetite.

Deutsch called the information-subpoena provision "a dangerous and vague loophole" that Internet pornographers and cyberstalkers could use to violate customers’ privacy. Verizon is working with lawmakers in an attempt to overturn the provision; earlier this month, Sen. Sam Brownback (R-Kan.) introduced a bill that would ban the RIAA’s use of information subpoenas to find music pirates.

"Bringing a few targeted enforcement cases was not enough for them," Deutsch said. "They wanted the right to get everyone’s name and go on a blitzkrieg approach to enforcement."

Sherman said the RIAA will fight to keep the provision in the federal law.

"We think that taking away the information-subpoena process is basically giving people the right to infringe with impunity," said Sherman, who once worked for Verizon as an information technology lawyer.

Sherman also hinted that settlements in the next wave of lawsuits could be higher than $3,000 each, because "the notion that ’Oh, I didn’t know this was illegal’ is less and less true," thanks to the onslaught of press coverage of the Sept. 8 suits.

## Music Industry Will Talk Before Suing

The music industry, criticized for its recent wave of lawsuits aimed at stopping song swapping on the Internet, agreed yesterday to contact future defendants before they are sued and give them a chance to pay a cash settlement or argue that they have been mistakenly accused of copyright infringement.

The shift, announced at a Senate hearing by Mitch Bainwol, chairman of the Recording Industry Association of America, was in response to critics who accused the music industry of casting too wide a legal net over alleged song pirates, ensnaring 12-year-olds and grandfathers alike.

"We are trying to be reasonable and fair and allow these cases the opportunity to be resolved without litigation," Bainwol said.

Bainwol nevertheless defended the industry's decision to file 261 lawsuits alleging copyright infringement. "The suits are the last resort and the end product of our campaign," he said. "They are the last thing we had in our quiver."

U.S. sales of recorded music, mostly compact discs, have dropped 31 percent drop over the past three years, the RIAA says. It blames people who trade songs on the Internet.

The RIAA has advertising and education campaigns to teach song-swappers about copyright law. It also is suing those it characterizes as "egregious offenders," mostly people with at least 1,000 songs on their computer hard drives that can be downloaded by others using peer-to-peer file-sharing software such as Kazaa, Grokster and Morpheus.

The lawsuits have been criticized by civil liberties groups, which say the RIAA's ability to use subpoenas to learn the names of traders is unconstitutional. Some members of Congress also have expressed concern. Sen. Norm Coleman (R-Minn.), who called yesterday's hearing of the Senate Permanent Subcommittee on Investigations, said in an interview last week that he hoped to find a way to protect copyrighted songs without suing consumers.

The Digital Millennium Copyright Act of 1998 gives copyright holders the right to subpoena Internet service providers for the names and addresses of people suspected of illegally trading song files. Bainwol said the RIAA subpoenas force the Internet service providers to give up only "the same information that some of the ISPs sell to their marketing partners."

Yesterday's hearing included celebrity witnesses - rappers LL Cool J and Chuck D, who are on opposite sides of the song-sharing debate and RIAA suits.

"A reporter asked me if I wanted to sue my fans," said LL Cool J, whose rap name stands for "Ladies Love Cool James" and who was referred to as "Mr. Cool J" by Coleman. "I told him, 'Do you write for your paper for free?' "

Chuck D, founding member of Public Enemy, an influential rap group, was one of the first musicians to support peer-to-peer file-sharing. His 1999 "There's A Poison Goin' On" was the first full-length album by a major artist made available for download.

"P2P to me means 'power to the people,' " Chuck D said. "The fans got hold of the technology before the industry did."

The hearing included a sharp exchange between Sen. Carl M. Levin (D-Mich.) and Alan Morris, executive vice president of Sharman Networks Ltd., Kazaa's parent company.

Kazaa is the most popular Internet file-sharing software and the bane of the music industry, which says Kazaa is the main enabler of song piracy and that it has knowingly built a business on violating copyrighted material. The company is incorporated in Australia and Vanuatu, a group of South Pacific islands that advertises itself as a tax haven. ("Just like Delaware," Morris said.) Levin pointed out that the island nation had been on a State Department list for money-laundering concerns and that Kazaa's refusal to name its owners made the company look suspicious.

Levin read from Kazaa's Web site, which says the service will revoke its

customers’ use of the software if it is used to violate copyright. But Morris acknowledged that the company does not know how its customers use the service.

"It’s an honor agreement," Morris said.

"But it’s not enforceable," Levin said.

"It’s not enforceable," Morris conceded.

"Would you enforce it if you could?" Levin persisted.

"If a court of due competence stated there had been an infringement," Morris said, "we would certainly look at it."

After the hearing, Levin said of Kazaa: "I think they must know that most of their downloads are violations of copyright. They are highly secretive and highly evasive."

Yesterday’s hearing also featured look at what it’s like to be sued.

Lorraine Sullivan said she found out she was being sued when she played her home voice mail on Sept. 9 and it contained messages from four reporters, asking her for reaction.

She called the RIAA and was referred to Patricia Benson, a lawyer for Los Angeles’s Mitchell Silberberg & Knupp LLP, one of the RIAA’s outside law firms. Sullivan testified that Benson told her it would probably cost between $3,000 and $4,000 to settle the suit, and that "nobody likes having to be the heavy."

Sullivan told Benson that she had $1,500 in her savings account and was a student with a part-time job. Sullivan said the lawyer asked her if she could get the money from her parents. No, Sullivan, replied. Anyone else? No, Sullivan said.

Benson finally asked: Do you have credit cards? Yes, Sullivan said, but they’re almost maxed out. Benson said she would ask the RIAA to accept a lesser payment. Two days later, Sullivan said she agreed to settle for $2,500.

"I won’t be buying any more" CDs, she testified.

## Ballmer Slams Hackers As Criminals, Not Innovators

Ask Microsoft CEO Steve Ballmer whether some hackers contribute to the IT industry, and you’ll get an emphatic, ’No!’"

"Hackers are criminals," Ballmer says, plain and simple. And they don’t innovate, either, he adds. "Hackers are people who are causing hundreds of millions and billions of dollars in damage," he says. "And they’re not showing that they are not all that smart and creative and clever."

In an exclusive interview conducted by VARBusiness in conjunction with sister publication CRN, Ballmer made it absolutely clear where his company - arguably the biggest target for cybercrime the world over - stands when it comes to hacking, be it malicious code-authoring or what

some consider to be ethical programming. Ballmer likens these individuals to criminals who blow up buildings and says the monetary damage is worse. And he takes umbrage with the notion that some are ethical and help to create new innovations for the market by pushing IT to its limits. Most, he notes, release their malicious code after patches for Microsoft software have been released, meaning that they are simply reverse engineering to exploit security weaknesses or holes in software.

Ballmer was responding to a question posed to him by the editors of VARBusiness, which collected a wealth of queries by its readers. In fact, the entire interview consisted of actual reader questions submitted by partners like you. In an upcoming issue, VARBusiness will publish the entire transcript of the question-and-answer session, which covered a variety of topics ranging from the inequity between what Microsoft gets for sales and its partners receive, how the software giant will combat Linux and other lower-cost alternatives, and how Microsoft defines opportunities in the SMB market. No topic, however, raised Ballmer’s level of passion quite like the issue of security, which he conceded has forced his company to respond in new ways.

"There’s no way to way to look these people as anything other than what they are: malicious people who are violating the law," Ballmer said. Their work, of course, is causing Microsoft significant grief.

"We’re really going to have to ratchet up our game in terms of working with our customers and our partners to work with our customers around security" he said. He added that the company is planning a significant announcement around security specifically to address the ongoing problem associated with malicious attacks on Microsoft systems and networks. Ballmer hinted that there will be a new set of ways Microsoft educates its customers on security and puts partners in position to help customers with theirs. "That is job one on a day-to-day on my radar," he said.

## Microsoft in $10.5 Million Software Sale Settlement

Microsoft Corp. said on Tuesday that it will pay $10.5 million to settle a class-action legal dispute with customers who bought software directly from the No. 1 software maker’s Web site.

The settlement, which is pending in the U.S. District Court in Maryland and must be approved by U.S. District Judge J. Frederick Motz, will pay each purchaser a portion of the price paid for software bought up until April 30, 2003.

## Microsoft Faces Class-Action on Security Breaches

Microsoft Corp. faces a proposed class-action lawsuit in California based on the claim that its market-dominant software is vulnerable to viruses capable of triggering "massive, cascading failures" in global computer networks.

The lawsuit, which was filed on Tuesday in Los Angeles Superior Court, also claims that Microsoft’s security warnings are too complex to be understood

by the general public and serve instead to tip off "fast-moving" hackers on how to exploit flaws in its operating system.

The suit claims unfair competition and the violation of two California consumer rights laws, one of which is intended to protect the privacy of personal information in computer data bases. It asks for unspecified damages and legal costs, as well as an injunction against Microsoft barring it from unfair business practices.

Many of the arguments in the lawsuit and some of its language echoed a report issued by computer security experts in late September, which warned that the ubiquitous reach of Microsoft’s software on desktops worldwide had made computer networks a national security risk.

That report presented to the Computer and Communications Industry Association, a trade group representing Microsoft’s rivals, said the complexity of Microsoft’s software made it particularly vulnerable.

Microsoft said it had received a copy of the lawsuit and that its lawyers were reviewing it, but could not comment immediately.

Dana Taschner, a Newport Beach, California, lawyer who filed the lawsuit on behalf of a single plaintiff and a potential class of millions of Microsoft customers, could not be immediately reached for comment.

"Microsoft’s eclipsing dominance in desktop software has created a global security risk," the lawsuit filed in Los Angeles said. "As a result of Microsoft’s concerted effort to strengthen and expand its monopolies by tightly integrating applications with its operating system ... the world’s computer networks are now susceptible to massive, cascading failure."

With some $49 billion in cash and more than 90 percent of the market in PC operating systems, Microsoft has long been seen as a potential target for massive liability lawsuits.

But the company, which has been moving to settle anti-trust claims that it abused its monopoly on PC software, has been also seen as shielded from liability claims by disclaimers contained in the licenses that users must agree to when installing software, according to experts.

The lawsuit comes in the wake of two major viruses that have recently taken advantage of flaws in Microsoft software.

Slammer, which targeted computers running Microsoft’s server-based software for databases, slowed down Internet traffic across the globe and shut down flight reservation systems and cash machines in the United States.

The Blaster worm, meanwhile, burrowed through hundreds of thousands of computers, destroying data and launching attacks on other computers.

Since early 2002 Microsoft has made computer security a top priority under a "Trustworthy Computing" initiative spearheaded by the company’s founder and Chairman, Bill Gates.

## OpenOffice 1.1 Ready For Downloading

OpenOffice.org, the open-source group of developers working on the free

OpenOffice suite of applications, beat Microsoft to the punch and released the final version of its 1.1 bundle on Wednesday.

OpenOffice 1.1, a competitor to Microsoft in the productivity suite space - Microsoft will release its newest edition, Office 2003, later this month - is available now for downloading in Windows, Linux, and Solaris editions.

Version 1.1 includes a word processor, spreadsheet, and presentation maker; includes one-click export of documents to Adobe's PDF format; sports an updated interface; offers enhanced support for Microsoft Office document formats; and loads faster than before, said OpenOffice.org.

"The release of Version 1.1 of OpenOffice.org is a major achievement for the OpenOffice.org community," said Curtis Sasaki, the vice president of Sun's desktop division. OpenOffice shares core code with Sun's branded StarOffice application suite.

Versions for Mac OS X, FreeBSD, and the x86 versions of Solaris are still under development, but will be available later this year, said the group.

OpenOffice 1.1 can be downloaded from the OpenOffice.org Web site.

## AOL Introduces New Spam Filters

America Online Inc. on Tuesday introduced new spam filters for members using AOL 8.0 Plus and which will be delivered in the coming months to members using AOL 8.0, AOL 7.0, AOL 6.0 and AOL for Mac OS X. The automatic delivery of these spam filters will be "seamless to members using earlier versions of the AOL software for Windows or AOL for Mac OS X and they will quickly see a noticeable difference in the number of spam e-mails they receive," said David Gang, executive vice president of AOL Products.

Previously available only to members using AOL 9.0 Optimized, the latest version of the AOL and AOL for Broadband services, these spam filters "learn" and adapt to the type of e-mail that each member considers to be spam. The filters require no additional software and no action on the part of members to install.

AOL receives reports of up to 10 million unwanted mails per day, mainly through the use of the "Report Spam" button that's available with AOL 8.0, AOL 8.0 Plus and AOL 9.0 Optimized. Reporting spam to AOL helps the software's spam filters get smarter as members use them, while enabling AOL's proprietary server-side anti-spam filters to adapt in real-time to the growing epidemic of junk e-mail from the Internet, the company said.

## Internet Guns for Hire: Best Pop-Up Killers

Even the most respectable businesses are not above planting those maddening pop-up ads that make visiting their Web sites a furious exercise in closing unwanted windows. That is why pop-up blockers, or killers, as they are affectionately known - a type of software that stops ads before they pop up - are such a hot item. A program that automatically blocks pop-up ads intelligently - meaning it can distinguish the "good" pop-ups from the

"bad" - is worth its weight in gold.

Alas, the selection of a pop-up blocker is not easy. Some block everything, requiring the user to tell them to allow pop-ups from certain sites. Others claim they are intelligent, but still wind up blocking the wrong pop-ups or letting "bad" pop-ups through. These programs also vary in their ability to thwart other advertising delivery techniques, such as Windows Messenger pop-ups. The following examines three of the leading programs available for wiping out the bane of Web surfers everywhere.

PopUpCop is one of the more effective programs in the category. It blocks pop-up ads intelligently and squelches unwanted Java applets and JavaScript, as well as 15 other techniques that advertisers use to get an Internet surfer’s attention. PopUpCop also blocks a category of spyware called "drive-by downloading," in which a site tries to load something onto a user’s PC via an ActiveX control.

PopUpCop does not use site-title or URL-address matching when figuring out what to block. Instead, it monitors the user’s interaction with the browser and blocks pop-ups according to a set of rules. For example, a simple rule would be that when a user clicks on something, the action should only produce one result, said Peter Eden, proprietor of EdenSoft. "Less sophisticated [pop-up blockers] will miss pop-ups that appear when leaving a Web site or closing the main browser window," Eden told NewsFactor. "To catch all of them requires a bit of a technical tap dance."

PopUpCop is packaged as an Internet Explorer add-in. Instead of being in the system tray, it resides in a customizable browser toolbar. "There are too many items in the system tray," Eden said. "System-tray implementations can be far less efficient from an engineering and performance point of view. That just means slower for the end-user."

The PopUpCop toolbar features an Internet irritation indicator and irritation-level slider that allow the user to control the blocking of different ad techniques.

Eden said that the company is considering enhancing PopUpCop by adding a feature to block adware, which usually arrives on people’s machines unnoticed when they install software for P2P file-sharing. "We’re probably going to start blocking adware but we will continue to advise people to remove it themselves," Eden said. EdenSoft also is considering adding the capability to block pseudo pop-ups that are written in active HTML.

PopUpCop sells for US$19.95.

One straightforward pop-up blocker is iHatePopups from Sunbelt Software, the makers of iHateSpam. iHatePopups blocks pop-up and pop-under ads and does not make any distinction between "good" pop-ups and "bad" pop-ups - everything is blocked.

"It’s simple, cheap, and we have done research about what people want," said Stu Sjouwerman, chief operating officer of Sunbelt Software. "You can go overboard with adding features to pop-up blockers. We give users 90 percent of the features that they need at an affordable price."

With iHatePopups, a CTRL-click feature enables the user to allow a particular pop-up to appear. Users also can "whitelist" a particular Web page by right clicking on it to allow all pop-ups from that page to appear.

iHatePopups notifies the user with a message or sound when a pop-up has

been blocked. It also provides a history and log report showing how many pop-ups it has blocked and where they are from, Sjouwerman told NewsFactor. In addition to pop-ups, it blocks spam sent via the Windows Messenger service. It also stops Javascript error messages on Web sites that sometimes can put the user in an endless loop, Sjouwerman said.

iHatePopups is available from Sunbelt for $9.95. And Dell is bundling it into a "privacy package" that includes iHateSpam and Pest Patrol, a spyware blocker.

PopSubtract from interMute is another straightforward pop-up blocker that is less than 300 KB in size, making it easily downloadable even over a dial-up modem. The program installs as a tool-tray icon. Clicking on it reveals the control panel that lets the user toggle filtering on and off and view statistics. A "test" button on the control panel sends users to a diagnostic Web site where they can test the program's performance and functionality.

PopSubtract boasts of what it calls "SmartPop logic," an ability to discern good pop-ups from bad. SmartPop works by examining the site from which a pop-up comes, said Brian Katzen, marketing manager for interMute. Secure sites (HTTPS), for example, are not filtered by default, so banking and stock-trading sites that use pop-ups in normal user transactions will not be blocked.

Additionally, SmartPop allows pop-up windows to open if they originate from a hyperlink, Katzen told NewsFactor. "If a hyperlink spawns a pop-up window, the window is not blocked," he said. However, if the hyperlink opens another browser window from a different Web site, PopSubtract will block it.

The PopSubtract statistics screen provides information on the number of pop-up ads blocked and the sites launching the ads. Trusted sites can be added to a whitelist by right clicking the blocked sites.

PopSubtract is available free on a trial basis and costs $19.95 for a one PC license.

Other programs are available. Some of the more notable ones not discussed here include PopNot, Popup Ad Filter, Popup Dummy!, and Popup XP. Since these programs will be an integral part of a user's Internet experience, it makes sense to examine them on a trial basis if the vendor allows it.

Pop-ups are annoying, but an bumbling pop-up killer may just add to the irritation.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.